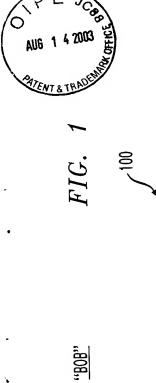


MacKENZIE 15 Serial No.: 10/600,687 Ryan, Mason & Lewis, LLP; W. E. Lewis (516) 759-2722



 $\begin{array}{lll} \sigma \leftarrow H(x, y, w) & \overbrace{\hspace{1cm}} & 118 \\ s_2, r_5, r_1', r_2', r_3', r_4' \stackrel{R}{\leftarrow} Z_q \stackrel{120}{\sim} 120 \\ E_5 \leftarrow (g^r5, (h_1)^r5x^e2 (vx^-(a_2+c_2\sigma)_y - (b_2+d_2\sigma)_s2) \\ \times (E_1)^-(a_2+c_2\sigma) \times (E_2)^-(b_2+d_2\sigma) \times (E_4)^s2 & \overbrace{\hspace{1cm}} & \vdots \\ E_1' \leftarrow (g^r1, (h_2)^r'1x^s2) \stackrel{126}{\sim} 126 \\ E_2' \leftarrow (g^r2, (h_2)^r'2y^s2) \stackrel{126}{\sim} 128 \\ E_2' \leftarrow (g^r3, (h_2)^r'3y^s2) \stackrel{120}{\sim} 130 \end{array}$ $E_4^{\prime} \leftarrow (g^{r4}, (h_2)^{r4}) \times (E_1^{\prime})^{-(a_2+c_2\sigma)} \times (E_2^{\prime})^{-(b_2+d_2\sigma)}^{-(b_2+d_2\sigma)}$

 $\langle E_1, E_2, E_3, E_4, \langle x, y, w, v \rangle \rangle$ $E_4 \leftarrow (g^r 4, (h_1)^r 4x^{-(a_1 + c_1 \sigma)} y^{-(b_1 + d_1 \sigma)})^{-112}$ $s_1, r_1, r_2, r_3, r_4 \stackrel{R}{\leftarrow} Z_q - 104$ $E_1 \leftarrow (g^{r_1}, (h_1)^{r_1} x^{s_1}) - 106$ $E_2 \leftarrow (g^{r_2}, (h_1)^{r_2} y^{s_1}) - 108$ $E_3 \leftarrow (g^{r_3}, (h_1)^{r_3} y^{s_1}) - 110$ $\sigma \leftarrow H(x, y, w)$

 $\langle E_5, E_1', E_2', E_3', E_4' \rangle$ $w \leftarrow x^{e_1} (vx^{-(a_1+c_1\sigma)}y^{-(b_1+d_1\sigma)})^{s_1} \cdot E_5[2] \cdot (E_5[1])^{-\beta_1}$



MacKENZIE 15 Serial No.: 10/600,687 Ryan, Mason & Lewis, LLP; W. E. Lewis (516) 759-2722

2/2

